(19)日本国特許庁（ＪＰ）　(12)公開特許公報(A)　(11)特許出願公開番号

特開平7－325785

(43)公開日　平成７年(1995)12月12日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　15/00	３３０　Ｂ	7459－5Ｌ		
Ｇ０９Ｃ　1/00		9364－5Ｌ		
Ｈ０４Ｌ　12/40				
			Ｈ０４Ｌ　11/00　３２０	

審査請求　未請求　請求項の数５　ＯＬ　（全７頁）

(21)出願番号　特願平6－121093

(22)出願日　平成６年(1994)６月２日

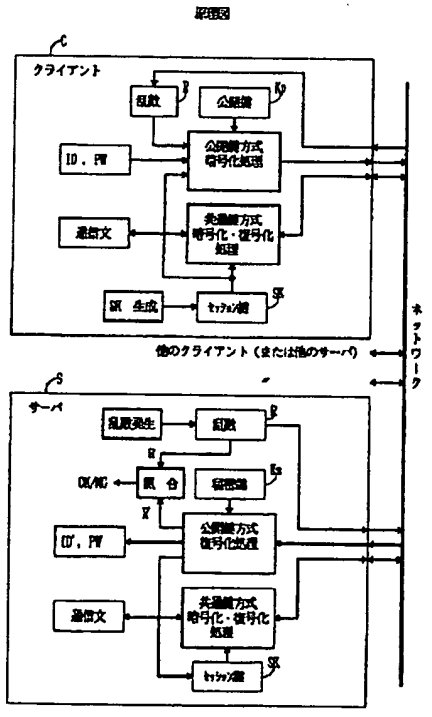
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地
(72)発明者　菊池　浩明
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　黒田　康嗣
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(74)代理人　弁理士　井桁　貞一

(54)【発明の名称】　ネットワーク利用者認証方法および暗号化通信方法とアプリケーションクライアントおよびサーバ

(57)【要約】

【目的】ネットワークのセキュリティを向上させる方法に関し、従来のパスワード認証方式と互換性をもち、暗号鍵の管理を安全・容易にし、利用者の個別追加・取消が容易であり、再送攻撃を無効にする。

【構成】利用者識別子ＩＤとパスワードＰＷとをクライアントから送信し、サーバは該当するＩＤとＰＷとが存在することを確認することで利用者認証を行うネットワークアプリケーションシステムにおいて、クライアントはＩＤとＰＷとを公開鍵方式のサーバの公開鍵Ｋｐで暗号化してサーバへ送信し、サーバは自分の秘密鍵Ｋｓでそれを復号化することによりＩＤとＰＷとを取り出す。また、認証の初めにサーバが乱数Ｒをクライアントに送信し、クライアントがＩＤとＰＷと受信した乱数Ｒとをふくめて公開鍵Ｋｐで暗号化してサーバへ送信し、サーバは、復号化した乱数Ｒ'が先に送信した乱数Ｒと同じであることを確認する。



1

【特許請求の範囲】

【請求項1】　利用者識別子（ＩＤ）とパスワード（ＰＷ）とをクライアント（Ｃ）からサーバ（Ｓ）へ送信し、サーバ（Ｓ）はファイルを参照して該当する利用者識別子（ＩＤ）とパスワード（ＰＷ）とが存在することを確認することで利用者認証を行うネットワークアプリケーションシステムにおいて、

クライアント（Ｃ）は、利用者識別子（ＩＤ）とパスワード（ＰＷ）とを公開鍵方式のサーバ（Ｓ）の公開鍵（Ｋｐ）で暗号化してサーバ（Ｓ）へ送信し、

サーバ（Ｓ）は自分の秘密鍵（Ｋｓ）でそれを復号化することにより、利用者識別子（ＩＤ'）とパスワード（ＰＷ'）とを取り出すことを特徴とするネットワーク利用者認証方法。

【請求項2】　認証の初めにサーバ（Ｓ）が乱数（Ｒ）をクライアント（Ｃ）に送信し、

クライアント（Ｃ）が利用者識別子（ＩＤ）とパスワード（ＰＷ）と受信した乱数（Ｒ）とをふくめて公開鍵（Ｋｐ）で暗号化してサーバ（Ｓ）へ送信し、

サーバ（Ｓ）は、復号化した乱数（Ｒ'）が先に送信した乱数（Ｒ）と同じであることを確認することを特徴とする請求項1に記載のネットワーク利用者認証方法。

【請求項3】　請求項1または請求項2に記載のネットワーク利用者認証方法において、クライアント（Ｃ）は共通鍵方式のセッション暗号鍵（ＳＫ）を発生させ、利用者識別子（ＩＤ）とパスワード（ＰＷ）と共に前記のセッション暗号鍵（ＳＫ）をふくめて公開鍵（Ｋｐ）で暗号化して送信し、

サーバ（Ｓ）、クライアント（Ｃ）共に、認証以後のセッション全体を前記のセッション暗号鍵（ＳＫ）に基づいて暗号化することを特徴とする暗号化通信方法。

【請求項4】　請求項1または請求項2に記載の利用者認証方法を用いるネットワークアプリケーションクライアントまたは請求項3に記載の暗号化通信方法を用いるネットワークアプリケーションクライアント。

【請求項5】　請求項1または請求項2に記載の利用者認証方法を用いるネットワークアプリケーションサーバ、または請求項3に記載の暗号化通信方法を用いるネットワークアプリケーションサーバ。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は多数の計算機が接続されているネットワーク環境において、セキュリティを向上させる方法に関する。

【０００２】近年の分散処理環境では、ネットワークを介して遠隔地にある計算機をあたかも直接接続されているかのように操作することのできる遠隔仮想端末アプリケーション（telnet）や、ファイル転送アプリケーション（ftp）などが広く利用されている。

【０００３】これらのネットワークアプリケーションは

2

商用化ネットワーク時代における計算機の遠隔保守作業や、ソフトウェアのオンライン流通などのサービスを実現する必須要素と考えられる。しかし、これらのネットワークアプリケーションは開放的なアーキテクチャに基づいて構築されており、通常、利用者認証方式として利用者識別子とパスワードとをそのまま転送するプロトコルを採用している。この場合は各種の監視装置などによる盗聴が比較的容易に行えてしまう。盗聴は即パスワードの盗難につながるため致命的である。

【０００４】

【従来の技術】これまで、パスワードによる認証に代わる方式として、暗号理論に基づく様々な認証方式が提案されている。なお、暗号方式には大別して共通鍵方式と公開鍵方式とがある。

【０００５】共通鍵方式は、送信側の暗号化鍵と受信側の復号化鍵とが同じ暗号鍵であり、その暗号鍵によって送信側で通信文（平文）を暗号化して送信し、受信側で受け取った通信文（暗号文）を同じ暗号鍵で復号化するものである。送信側、受信側共に暗号鍵を秘密に管理しておかなければならない。秘密鍵方式、慣用暗号方式ともいう。

【０００６】公開鍵方式は、送信側の暗号化鍵と受信側の復号化鍵とが異なった暗号鍵であり、一方（公開鍵）を公開し、他方（秘密鍵）を秘密にするものである。暗号化認証方式の例を以下に示す。

①　認証サーバを設け、クライアントは認証サーバからチケットを発行してもらい、そのチケットを共通鍵方式により暗号化してアプリケーションサーバに送ることで認証する方式。

②　公開鍵方式により、各利用者が自分専用の秘密鍵と公開鍵とを生成して秘密鍵を管理し、公開鍵を公開ファイルに登録しておき、自分の秘密鍵によりメッセージ（パスワード）を暗号化して送り、サーバは公開ファイルから利用者の公開鍵を取り出して復号化して検査する、電子署名を利用してサーバが利用者を認証する方式。

【０００７】これらの他にも、零知識証明を用いるもの、公開鍵として意味のある識別子を用いるもの等さまざまな試みが提案されている。しかし、これらの方式は、従来のネットワークアプリケーションと互換性がなく、実際に適用するには、大きな変更が必要である。例えば①では、認証サーバが別に必要であり、利用者はアプリケーションサーバの他に認証サーバとも通信しなければならないこと、②では全利用者がそれぞれ秘密鍵をもち、公開鍵を登録しなければならないこと、かつ、その秘密鍵を安全に管理すること等が必要である。

【０００８】特に、組織間接続等の応用場面においては、セキュリテイを必要とする利用者は限られており、従来のネットワークアプリケーションとも併用することが多いことを考慮すると、これらの変更は大きな負担と

なりうる。また操作方法が大幅に変わるのは利用者にとって抵抗感を生じさせることにもなる。

【0009】そこで、従来のパスワード認証に暗号技術を適用してセキュリテイを強化する方法が提案されている。これは、利用者識別子とパスワードを含むセッションをまるごと共通鍵暗号で暗号化するというものである。しかし、その際用いられる暗号鍵をどう管理するか、という問題が残されている。

【0010】例えば、ある利用者が一時的に他の組織（研究組合等）に属し、WANを経由して元の組織（本来の所属）のLANにアクセスする場合を考える。この場合、利用者は、他の組織の計算機を利用してネットワークアプリケーションを利用するので、その計算機のファイル内に暗号鍵などの重要な情報を蓄えるのは危険である。その計算機の管理者になりすまして他者がファイルの内容を強制的に読み出すことが可能であるためである。

【0011】一般に、一つのサーバに対してクライアントは多数存在する。つまり、WANを経由してアクセスする利用者も多いということである。これらの利用者全てに共通の暗号鍵を与えると、だれかが暗号鍵を漏らしたりすれば、その影響は全員におよぶ。また、その内の一人でも、利用者資格が無くなればそのサーバの利用者全部に新しい暗号鍵を再配付しなければならない。利用者毎に別の暗号鍵を作って管理するのはサーバの負担が大である。また、利用者は多数のサーバにアクセスする可能性がある。サーバごとに秘密の暗号鍵があると利用者にとって、その管理がさらに面倒になる。

【0012】一方、ネットワーク上の不正行為としては、情報を盗み出す「盗聴」の他に、ネットワークに妨害を与える「攻撃」がある。特に攻撃のなかには再送攻撃というものがある。これは、たとえ通信文が暗号化されていても、盗聴によりそのセッションを取り出しそのまま記憶しておき、後で再びサーバにそのまま送信することでクライアントになりすまし、サーバの混乱を招くというものである。この再送攻撃に対する対策も必要である。

【0013】

【発明が解決しようとする課題】本発明は、ネットワークアプリケーションにおいて、

① 従来のパスワード認証方式と互換性をもち、

② クライアントにおける暗号鍵の管理を安全・容易にし、

③ 利用者の個別追加・取消が容易であり、

④ 再送攻撃を無効にするようなセキュリテイ対策を目的としている。

【0014】

【課題を解決するための手段】図1は本発明の原理図である。

請求項1の発明：　利用者識別子ＩＤとパスワードＰＷとをクライアントＣからサーバＳへ送信し、サーバＳはファイルを参照して該当する利用者識別子ＩＤとパスワードＰＷとが存在することを確認することで利用者認証を行うネットワークアプリケーションシステムにおいて、クライアントＣは、利用者識別子ＩＤとパスワードＰＷとを公開鍵方式のサーバＳの公開鍵Ｋｐで暗号化してサーバＳへ送信し、サーバＳは自分の秘密鍵Ｋｓでそれを復号化することにより、利用者識別子ＩＤ’とパスワードＰＷ’とを取り出す。

【0015】請求項2の発明：　請求項1の発明において、認証の初めにサーバＳが乱数Ｒをクライアント Ｃに送信し、クライアントＣが利用者識別子ＩＤとパスワードＰＷと受信した乱数Ｒとをふくめて公開鍵Ｋｐで暗号化してサーバＳへ送信し、サーバＳは、照合により、復号化した乱数Ｒ’が先に送信した乱数Ｒと同じであることを確認する。

【0016】請求項3の発明：　ネットワークアプリケーションシステムにおいて、クライアントＣは共通鍵方式のセッション暗号鍵ＳＫを発生させ、請求項1または請求項2の発明によって、利用者識別子ＩＤとパスワードＰＷと共に前記のセッション暗号鍵ＳＫをふくめて公開鍵Ｋｐで暗号化して送信し、サーバＳ、クライアントＣ共に、認証以後のセッション全体を前記のセッション暗号鍵ＳＫに基づいて暗号化する。

【0017】請求項4の発明：　ネットワークアプリケーションクライアントにおいて、請求項1または請求項2に記載の利用者認証方法を用いる。または請求項3に記載の暗号化通信方法を用いる。

【0018】請求項5の発明：　ネットワークアプリケーションサーバにおいて、請求項1または請求項2に記載の利用者認証方法を用いる、または請求項3に記載の暗号化通信方法を用いる。

【0019】

【作用】

請求項1の発明：　クライアントＣは、利用者識別子ＩＤとパスワードＰＷとを公開鍵方式のサーバＳの公開鍵Ｋｐで暗号化してサーバＳへ送信する。従って通信路上には秘密情報であるパスワードＰＷはそのまま現れることはない。

【0020】サーバＳは自分の秘密鍵Ｋｓでそれを復号化することにより、利用者識別子ＩＤ’とパスワードＰＷ’とを取り出す。これらの利用者識別子ＩＤ’とパスワードＰＷ’とは正しく暗号化・復号化されているなら、クライアントＣで暗号化される前の利用者識別子ＩＤとパスワードＰＷと一致するはずである。従って、利用者認証には、従来通り、ファイルに該当する利用者識別子ＩＤとパスワードＰＷが存在するかどうかをチェックすればよい。

【0021】請求項2の発明：　認証の初めにサーバＳが送信した乱数Ｒが、公開鍵Ｋｐで暗号化されてサーバ

5

Sへ戻ってくる。これを復号化した乱数R'が先に送信した乱数Rと同じであることを確認することにより、利用者認証を確実にすることができる。すなわち、盗聴により前回の内容を使って再送攻撃をしても乱数Rが異なっているので無効である。

【0022】請求項3の発明：　クライアントCは乱数等に基づいて共通鍵方式のセッション暗号鍵SKを発生させ、請求項1または請求項2の発明によって、利用者識別子IDとパスワードPWと共に公開鍵Kpで暗号化して送信する。クライアントC、サーバS共に、認証以後のセッション全体を前記のセッション暗号鍵SKに基づいて暗号化する。これにより、通信文が暗号化される。かつ、そのセッション暗号鍵SKはそのセッション限りのものであって、クライアントC、サーバS共に、保存・管理する必要がない。

【0023】

【実施例】以下、図面を参照して本発明の実施例を説明する。図2は本発明の実施例のサーバ、およびクライアントの構成図を示す。

【0024】アプリケーションシステムは、クライアントとなる端末（ワークステーション、パーソナルコンピュータ等）とサーバとなる計算機（汎用機、ワークステーション、パーソナルコンピュータ等）とがネットワークで結合されたハードウェアと、クライアントで実行されるクライアントプログラムCPと、サーバで実行されるサーバプログラムSPとからなる。サーバプログラムSP（およびクライアントプログラムCP）は複数ある場合があり、それぞれが別のハードウェア（計算機）上にあってもよいし、同一のハードウェア上にあってもよい。以下1つのアプリケーションについてハードウェアとプログラムとを一体にしてクライアントC、サーバSと呼ぶ。利用者は個々に利用者識別子IDとパスワードPWとをもつ。

【0025】クライアントCは、ネットワーク間通信を制御する通信処理部14、ユーザインタフェース（入力部）18、認証情報（利用者識別子IDとパスワードPW他）を暗号化する公開鍵方式暗号化処理部11、サーバSの秘密鍵Ksに対応する公開鍵Kpを管理する公開鍵データベース（サーバが複数ある場合である。図示はしてない。）、取り出した公開鍵Kpを保持する公開鍵格納部12、サーバSから受信した乱数Rを格納する乱数格納部13、要求したサービスの実行を行うサービス実行部（図示してない）、セッション鍵SKを生成するセッション鍵生成部16、セッション鍵SKを保持するセッション鍵格納部17、セッションの暗号化・復号化を行う共通鍵方式暗号化・復号化処理部15、全体を制御する統括制御部（図示してない）からなる。

【0026】サーバSは、ネットワーク間通信を制御する通信処理部24、認証情報を復号化する公開鍵方式復号化処理部21、秘密鍵Ksを保持する秘密鍵格納部22、クライアントCへ送信する乱数Rを生成する乱数生成部26、乱数Rを保持する乱数格納部23、乱数Rと受信して復号化した乱数R'とを照合する乱数照合部29、全利用者の利用者識別子IDと、パスワードPWとを管理するID/PWファイル30、パスワード照合部28、要求されたサービスの実行を行うサービス実行部（図示してない）、セッションの暗号化・復号化を行う共通鍵方式暗号化・復号化処理部25、全体を制御する統括制御部（図示してない）からなる。

6

【0027】暗号方式としては、公知の方式を使用すればよい。例えば、認証情報の暗号化には公開鍵方式暗号RSAを、セッションの暗号化には共通鍵方式暗号DESのCFB64運用モードを用いる。

【0028】以下に図3のプロトコル説明図によって、動作手順を説明する。

ステップ1：クライアントCはサーバSへ認証要求を送信する。

ステップ2：サーバSは乱数Rを生成し、クライアントCへ返信する。

【0029】ステップ3：クライアントCはセッション鍵SKをランダムに生成し、IDとPWとサーバSから送られた乱数Rと共に、サーバSの公開鍵Kpで暗号化して、サーバSへ送信する。

【0030】ステップ4：サーバSは、受信した暗号化データを自身の秘密鍵Ksで復号化して利用者識別子ID'、パスワードPW'を取り出す。

ステップ5：サーバSは、R'がステップ2で送信したRと同一であるかを確認し、ID'、PW'が内部データベースに登録されているかを確認し、その結果をクライアントCへ通知する。

【0031】ここまでが認証のステップであり、ステップ5で異常がなければセッションに入る。

ステップ6：以後のセッションは、全体がセッション鍵SKで暗号化されており、クライアントCとサーバSは共にセッション鍵SKで暗号化した情報を送り、受け取った情報をセッション鍵SKで復号化する。

【0032】ここで、利用者からみたインタフェースは、IDとPWとを入力するだけであり、従来のパスワード認証と変わりはない。またアプリケーションの変更も小さなもので済む。

【0033】本実施例では、秘密情報PWはサーバSの他には利用者が記憶しているだけであり、通信路上では暗号化されている。サーバSの秘密鍵はサーバSがもっているだけであり、通信路には現れない。クライアントCまたは途中に入る計算機、監視装置等には、サーバSの公開鍵（これは秘密情報ではない）が残るだけで秘密情報は残らない。利用者の追加や取消し等はサーバSのデータベース（ファイル）を変更することにより行えばよく、他の利用者に影響が生じることはない。なお、サーバSのファイルに蓄積されている利用者認証情報（秘

密情報ＰＷを含む）が盗まれる可能性があるが、これは、別途、暗号化してファイルしておき、認証時に復号化して使用するようにすればよい。

【００３４】始めに（ステップ２）サーバＳからクライアントＣに乱数Ｒが送信されるが、この値はサーバＳで決められ、かつ毎回異なった値が用いられるため、たとえ第三者がネットワークに流れる暗号化認証情報を盗聴して記録しておき、後でクライアントＣになりすましてサーバＳに送る、いわゆる再送攻撃を試みても成功する確率は無視できるほど小さくできる。

【００３５】認証時にクライアントＣが任意に生成したセッション鍵ＳＫをサーバＳに渡し、以後のセッション全体を共通鍵方式で暗号化して通信するため、盗聴や改ざんを防止することができる。なお、セッション鍵ＳＫは毎回異なっており、また、それをサーバＳに渡すときには、サーバＳの公開鍵Ｋｐで暗号化しているので、サーバＳの秘密鍵Ｋｓがない限りセッション鍵ＳＫを解読される可能性は非常に少ない。

【００３６】

【発明の効果】以上説明したように、本発明によれば、利用者からみたインタフェースは、利用者識別子ＩＤとパスワードＰＷとを入力するだけであり、従来のパスワード認証と変わりはない。またアプリケーションの変更も小さなもので済む。

【００３７】本発明では、秘密情報ＰＷはサーバＳの他には利用者が記憶しているだけであり、通信路上では暗号化されている。サーバＳの秘密鍵Ｋｓはサーバ Ｓがもっているだけであり、通信路には現れない。クライアントＣまたはネットワークの途中に入る計算機、監視装置等には、サーバＳの公開鍵Ｋｐ（これは秘密情報ではない）が残るだけで秘密情報は残らない。従って、暗号鍵の管理が容易であり、安全である。

【００３８】利用者の追加や取消し等は、従来と同様に、サーバＳのデータベースを変更することにより行えばよく、他の利用者に影響が生じることはない。本発明の第２の発明では、始めに（実施例のステップ２）サーバＳからクライアントＣに乱数Ｒが送信される。この値はサーバＳで決められ、かつ毎回異なった値が用いられるため、たとえ第三者がネットワークに流れる暗号化認証情報を盗聴して記録しておき、後でクライアントになりすましてサーバに送る、いわゆる再送攻撃を試みても成功する確率は無視できるほど小さくできる。

【００３９】本発明の第３の発明では、認証時にクライアントＣが任意に生成したセッション鍵ＳＫをサーバに渡し、以後のセッション全体を暗号化して通信するため、盗聴やかいざんを防止することができる。なお、セッション鍵ＳＫは毎回異なっており、また、それをサーバＳに渡すときには、サーバＳの公開鍵Ｋｐで暗号化しているので、サーバＳの秘密鍵Ｋｓがない限りセッション鍵ＳＫを解読される可能性は非常に少ない。

【図面の簡単な説明】

【図１】　原理図

【図２】　実施例の構成図

【図３】　実施例のプロトコル説明図

【符号の説明】

ＩＤ，ＩＤ’　利用者識別子

ＰＷ，ＰＷ’　パスワード

Ｒ，Ｒ’　乱数

Ｋｐ　公開鍵

Ｋｓ　秘密鍵

ＳＫ　セッション鍵

Ｃ　クライアント　　Ｓ　サーバ

11　公開鍵方式暗号化処理部　　21　公開鍵方式復号化処理部

12　公開鍵格納部　　22　秘密鍵格納部

13　乱数格納部　　23　乱数格納部

14　通信処理部　　24　通信処理部

15　共通鍵方式暗号化・復号化処理部　　25　共通鍵方式暗号化・復号化処理部

16　セッション鍵生成部　　26　乱数生成部

17　セッション鍵格納部　　27　セッション鍵格納部

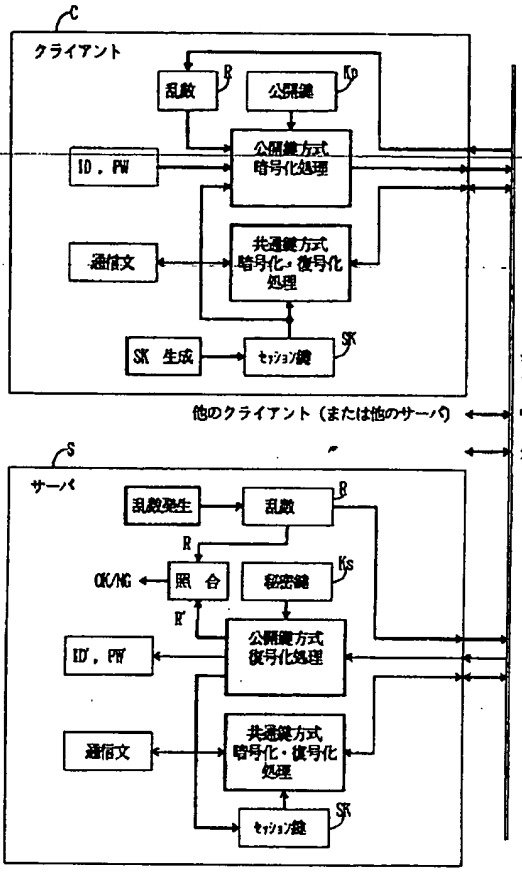
18　ユーザインタフェース部　　28　パスワード照合部

29　乱数照合部

30　ＩＤ／ＰＷファイル

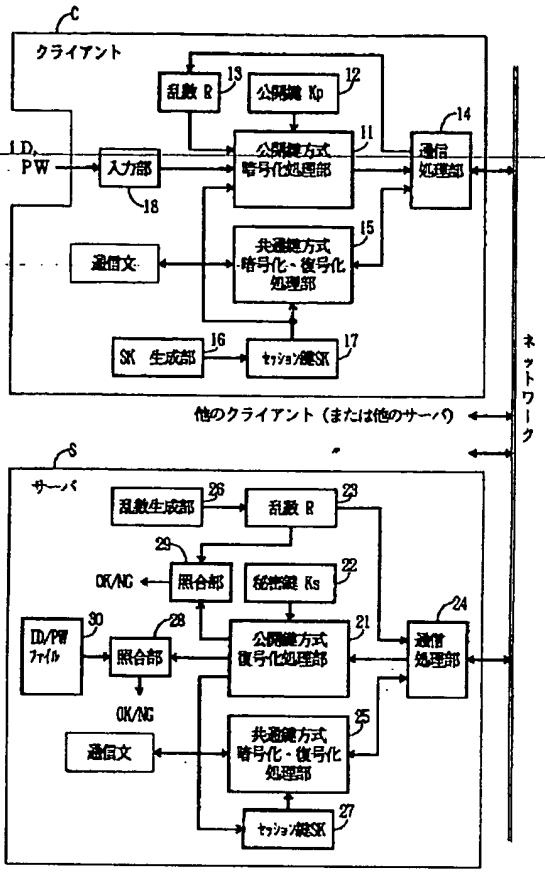
【図1】

原理図

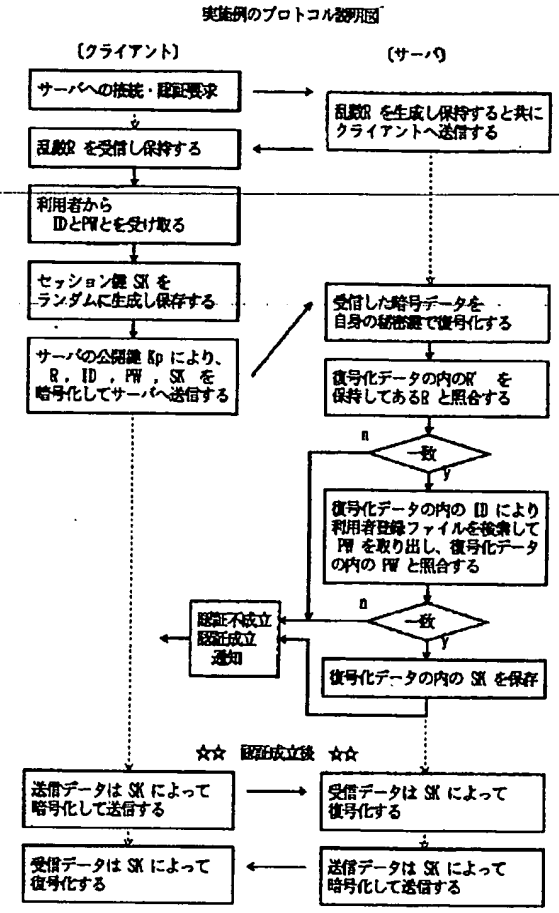


【図2】

実施例の構成図



【図3】


実施例のプロトコル説明図
〔クライアント〕
〔サーバ〕
サーバへの接続・認証要求
乱数R を生成し保持すると共にクライアントへ送信する
乱数R を受信し保持する
利用者から IDとPWとを受け取る
セッション鍵 SK を ランダムに生成し保存する
受信した暗号データを 自身の秘密鍵で復号化する
サーバの公開鍵 Kp により、 R，ID ，PW ，SK を 暗号化してサーバへ送信する
復号化データの内のR' を 保持してあるR と照合する
n
一致
y
復号化データの内の ID により 利用者登録ファイルを検索して PW を取り出し、復号化データの内の PW と照合する
n
一致
y
認証不成立 認証成立 通知
復号化データの内の SK を保存
☆☆ 認証成立後 ☆☆
送信データは SK によって 暗号化して送信する
受信データは SK によって 復号化する
受信データは SK によって 復号化する
送信データは SK によって 暗号化して送信する

Reference 3

Japanese Patent Application Public-disclosure No. 7-325785
Japanese Patent Application Public-disclosure date: December 12, 1995
Title of the invention: Method for authenticating a network user, encrypted communication method, application client and server
Japanese Patent Application No. 6-121093
Japanese Patent Application date: June 2, 1994
Applicant: Fujitsu Ltd.
Inventors: Hiroaki Kikuchi and Yasutsugu Kuroda

[Means for solving the problems]

Fig. 1 is a diagram illustrating a principle of the present invention.

Invention of Claim 1: In a network application system wherein client C transmits user identifier ID and password PW to server S, which verifies by referring to a file that the corresponding ID and PW actually exist, thereby authenticating the user, the client C encrypts the user identifier ID and password PW with public key Kp of the server S according to a public key system, and sends the encrypted ID and PW to the server S, and the server S decrypts the ID and PW using their own secret key Ks to extract user ID′ and password PW′.

Invention of Claim 2: In the invention of Claim 1, the server S sends random number R to the client C at the beginning of authentication, and the client C encrypts the user identifier ID, password PW and received random number R with the public key Kp and transmits the encrypted ID, PW and R to the server S, which verifies, by comparing decrypted random number R′ against the random number R, that the decrypted random number R′ is truly the previously transmitted random number R.

[Embodiment]

Hereafter, an embodiment of the present invention will

be described with reference to the attached drawings. Fig. 2 is a schematic diagram illustrating a server and client of the embodiment of the present invention.

An application system consists of: hardware comprising a terminal as a client (workstation, personal computer or the like) and a computer as a server (general purpose machine, workstation, personal computer or the like), the terminal and the computer being coupled via a network; client program CP to be executed by the client; and server program SP to be executed by the server. There are often multiple server programs SP (and client programs CP), which may be stored in different hardware (different computers) or in the same hardware. Hereafter, hardware and (a) client program(s) and hardware and (a) server program(s) will be respectively considered as a single unit for each application and referred to as client C and server S respectively. Each user has his (her) own user identifier ID and password PW.

The client C comprises: a communication processing section 14 for controlling communications between networks; a user interface (input section) 18; a public key system encryption processing section 11 for encrypting authentication information (user identifier ID and password PW or the like); a public key database for managing public keys Kp corresponding to secret keys Ks of servers S (applicable when there are multiple servers S, which is not depicted in the drawing); a public key storage section 12 for storing extracted public key Kp; a random number storage section 13 for storing random number R received from the server S; a service execution section for executing requested service (not indicated in the drawing); a session key generation section 16 for generating a session key SK; a session key storage section 17 for storing a session key SK; a secret key system encryption/decryption processing section 15 for encrypting/decrypting a session; and a centralized control section (which is not indicated in the drawing) for controlling the entire system.

The server S comprises: a communication processing section

24 for controlling communications between networks; a public key system decryption processing section 21 for decrypting authentication information; a secret key storage section 22 for storing a secret key Ks; a random number generation means 26 for generating a random number R to be sent to the client C; a random number storage section 23 for storing a random number R; a random number checking section 29 for comparing the random number R against a received and decrypted random number R'; an ID/PW file 30 for managing all users' user identifiers IDs and passwords PWs; a password checking section 28; a service execution section for executing requested service (not indicated in the drawing); a secret key system encryption/decryption processing section 25 for encrypting/decrypting a session; and a centralized control section (not indicated in the drawing) for controlling the entire system.

As an encryption system, a publicly known system can be employed. For example, a public key system encryption RSA may be employed to encrypt authentication information and a CFB64 application mode of a secret key system encryption DES may be employed to encrypt a session.

Hereafter, an operation procedure will be described by means of the protocol schematic diagram in Fig. 3.

Step 1: The client C transmits an authentication request to the server S.

Step 2: The server S generates a random number R and sends the random number R back to the client C.

Step 3: The client C randomly generates a session key SK, encrypts the session key SK together with ID, PW and random number R sent from the server S by the public key Kp of the server S, and transmits them to the server S.

Step 4: The server S decrypts the received encrypted data using their own secret key Ks and extracts user identifier ID' and password PW'.

Step 5: The server S checks to see whether R' is identical to the random number R sent at Step 2 and whether ID' and PW' are

registered in the internal database and notifies the client C of the result.

The above-described procedure from Step 1 through Step 5 is an authentication procedure and if it is verified at Step 5 that R' is identical to R and that ID' and PW' are registered, the operation proceeds to the next step for "session".

[Brief explanation of the drawings]

Fig. 1 is a principle diagram.

Fig. 2 is a schematic diagram illustrating a constitution of an embodiment of the present invention.

Fig. 3 is a diagram illustrating a protocol of the embodiment of the present invention.

[Description of referential symbols]

ID, ID': user identifier
PW, PW': password
R, R': random number
Kp: public key
Ks: secret key
SK: session key
C: client
S: server
11: public key system encryption processing section
12: secret key storage section
13: random number storage section
14: communication processing section
15: secret key system encryption/decryption processing section
16: session key generation section
17: session key storage section
18: user interface section
21: public key system
22: secret key storage section
23: random number storage section
24: communication processing section
25: secret key system encryption/decryption processing section

26: random number generation section
27: session key storage section
28: password checking section
29: random number checking section
30: ID/PW file